REMARKS

Please reconsider this application in view of the following remarks. Applicants thank the Examiner for carefully considering the application.

Disposition of Claims

Claims 1-3, 8, 11-15, 17-19, 22, and 23 are pending in the present application. Claims 1, 8, and 12 are independent. The remaining claims depend, directly or indirectly, from claims 1, 8, and 12.

Drawings

Applicants, again, respectfully request that the Examiner indicate in the next action whether the drawings filed on July 25, 2003 as amended in the Response to Office Action filed on March 12, 2007 are accepted.

Rejection(s) under 35 U.S.C. § 102

Claims 1-3, 8, 11-15, 17-19, 22, and 23 stand rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent Pub. No. 2004/0003251 (hereinafter referred to as "Narin"). This rejection is respectfully traversed.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP § 2131 (quoting *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2

USPQ2d 1051, 1053 (Fed. Cir. 1987)). Further, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." MPEP § 2131.

Independent claim 1 recites, in part,

> receiving a first certificate of a first server by a second server;
> storing said first certificate of said first server in a first trusted partner list accessible by said second server;
> receiving a second certificate of said second server by said first server; and
> storing said second certificate of said second server in a second trusted partner list accessible by said first server.

Claim 1 clearly requires that a second server receives and stores the certificate of a first server in a first trusted partner list, and that the first server receives and stores the certificate of the second server in a second trusted partner list. In other words, claim 1 requires that two servers each store the certificate of the other.

The Examiner asserts that Narin teaches the above limitations, stating that Narin discloses "two corporation servers (Figure 11) [that] establish a trust relationship ([0096]) by receiving and storing the public key certificates ([104]) of the other corporation server in their trusted identity server lists (Figure 11 & [0097])." *See* Office Action dated September 12, 2007 at page 3. The portion of Narin relied on by the Examiner does indeed disclose two corporation *DRM* servers that each receive and store a public key certificate of a corporation *identity* server of the other corporation.

Specifically, Figure 11 of Narin shows four servers: Corporation A Identity Server (1102), Corporation B Identity Server (1104), Corporation A DRM Server (1106), and Corporation B DRM Server (1108). Further, the Corporation A DRM Server (1106) stores the public key certificate of the Corporation A Identity Server (1102) and the public key certificate of the Corporation B Identity Server (1104) in its Trusted Identity Server List (1110). Similarly, the Corporation B DRM Server (1108) stores the public key certificate of the Corporation A Identity Server (1102) and the public key certificate of the Corporation B Identity Server (1104) in its Trusted Identity Server List (1112). *See* Narin, paragraphs [0095]-[0097]. However, the identity servers do not store the certificates of the DRM servers. Nor does either DRM server store the certificate of the other. In other words, Narin does not disclose two servers that each receive and store the certificate of the other as required by claim 1.

Claim 1 further requires that client access to a resource associated with the first server is controlled as a function of the trusted partner list of the second server. Narin very clearly teaches that a DRM server controls access to its published content using its own list of trusted identity servers. *See* Narin, paragraphs [0095]-[0098]. Narin is completely silent regarding access to content on one DRM server being controlled as a function of a list of trusted identity servers maintained by another DRM server or any other server. Accordingly, Narin cannot possibly be read to teach the above cited limitations of claim 1.

Independent claim 8 recites, in part,

> initiating use of a resource associated with a relying server by a client, wherein an authentication assertion reference is provided by said client to said relying server, and wherein said authentication assertion reference is provided to said client by an issuing server; ...
> *sending an authentication request comprising a certificate of said relying server to said issuing server;...*
> *sending an authentication assertion,* indicating that said client has been authenticated, *from said issuing server to said relying server* when

> said certificate is contained in said trusted partner list of said issuing server.

Emphasis added. Claim 8 recites a method of providing a circle of trust that involves two separate and distinct servers: a relying server and an issuing server. The method specifically requires the relying server to send an authentication request to the issuing server that includes the certificate of the relying server, and the issuing server to send an authentication assertion to the relying server when the certificate of the relying server is in the trusted partner list of the issuing server.

In contrast, as noted by the Examiner, Narin teaches a process for issuing a license in which a "DRM server [that] determines whether the identity certificate was issued by a[n] identity server in the trusted domain ([0117])...if the identity certificate is in the trusted domain, a license is granted to the requestor." *See* Office Action dated September 12, 2007 at page 5; *see* also, Narin at paragraph [0117] and Figure 5A. More specifically, Narin discloses that identity certificates are issued by identity servers. *See e.g.*, Narin at Fig. 10. Narin further discloses that when a user wants a license to access content, the user sends an identity certificate to a DRM server to request the license. *See e.g.*, Narin at paragraphs [0057], [0117] and Figure 5A. The DRM server then determines if the identity certificate is in its set of trusted certificates. *See e.g.*, Narin at paragraphs [0063] and Figure 5A. If the identity certificate is in the DRM server's set of trusted certificates, the DRM server then issues the requested license to the user. *See e.g.*, Narin at paragraphs [0064] and Figure 5A. At no point in this license issue process does the DRM server interact with the server that issued the identity certificate, *i.e.*, the identity server.

Accordingly, Narin cannot possibly be read to disclose a method in which a relying server sends an authentication request to an issuing server that includes the certificate of the relying server, and the issuing server sends an authentication assertion to the relying server when the certificate of the relying server is in the trusted partner list of the issuing server as required by claim 8.

In view of the above, independent claims 1 and 8 are not anticipated by Narin under 35 U.S.C. § 102(e). Independent claim 12 contains at least some similar limitations to those of claim 1 and is allowable for at least the same reasons as claim 1. Further, claims 2, 3, 11, 13-15, 17-19, 22 and 23 depend directly or indirectly from claims 1, 8, and 12, and are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is requested.

Conclusion

Applicants believe this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 03226/503001)

Dated: December 7, 2007

Respectfully submitted,

By /Robert P. Lord/
Robert P. Lord
Registration No.: 46,479
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicants